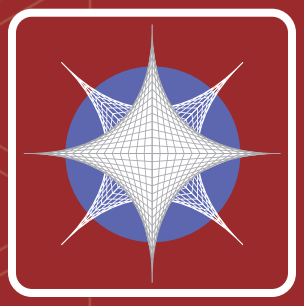


FORTINET

FortiOS™ Handbook - Fortinet Security Fabric

VERSION 5.6.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

4/26/2018

FortiOS™ Handbook - Fortinet Security Fabric

01-562-453730-20180426

TABLE OF CONTENTS

Change log

Date	Change description
October 16, 2017	Initial release

About this guide

The Fortinet Security Fabric is an end-to-end security solution that gives you control, integration, and easy management of security across your entire organization. The Security Fabric provides an intelligent architecture that interconnects discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire enterprise attack surface.

This document is a complete reference guide for the Security Fabric, including an overview of what the Security Fabric is, what devices are included in the Security Fabric and how they work together to secure your network, and how to configure and manage the Security Fabric.

What's new in the Security Fabric

This section contains a list of new features and enhancements for the Security Fabric.

FortiOS version 5.6.2

There are no new features for the Security Fabric in FortiOS version 5.6.2.

FortiOS version 5.6.1

FortiOS version 5.6.1 includes the following new features and enhancements for the Security Fabric.

FortiTelemetry support for IPsec VPN interfaces

You can now enable FortiTelemetry on IPsec VPN interfaces, and the Security Fabric can then detect the downstream FortiGate through the IPsec VPN interface. This allows you to send FortiTelemetry communication over a Gateway-to-Gateway IPsec VPN tunnel between two remote networks.

Redesigned Security Fabric menu

An updated GUI menu consolidates the Security Fabric features in one location. The new Security Fabric menu includes options for Physical Topology, Logical Topology, Audit, and Settings.

Security Fabric settings page improvements

The Security Fabric settings page is updated to be a centralized location where you can enable connectivity to other Fortinet products. The former **Enable Security Fabric** option is replaced by a **FortiGate Telemetry** option, which is what you use to enable the Security Fabric. The former **Downstream FortiGates** field is replaced by a **Topology** field, which shows a hierarchical map view of the FortiGates that are connected to the root FortiGate.

Security Fabric dashboard widget improvements

The Security Fabric dashboard widget is updated to include more Fortinet products. You can hover over the FortiGate icon to see the overall status of FortiTelemetry, and hover over the other icons to see the status of various devices in the Security Fabric.

The Security Fabric Score widget shows the Security Fabric Audit score and a list of the number of checks that were not passed, ranked by severity (Critical, High, Medium, and Low). Clicking on the widget and selecting **View/apply recommendations in Security Fabric Audit**, takes you to the Security Fabric Audit page.

Security Fabric topology page improvements

The Physical and Logical Topology pages include the following improvements:

- Updated Security Fabric legend
- New option to minimize the Topology: You can now show or hide areas of your organization's topology using the plus and minus signs beside the device icons in the topology pages. This makes it easier for you to view your organization's entire topology, or hide some areas of the topology to focus on other areas.
- New resource information alerts: The Security Fabric topology now shows CPU Usage and Memory Usage alerts in the device information tooltip. It also displays a warning if the FortiGate is in conserve mode.

SD-WAN support and improvements

The Security Fabric now supports SD-WAN by including SD-WAN information in the Security Fabric topology, and adds SD-WAN monitoring support.

The Security Fabric topology now includes SD-WAN information. Enhancements include greater visibility into where the data comes from and goes to, link saturation indicators, and detailed tooltip explanations.

The Security Fabric now retrieves monitoring information from all devices in the Security Fabric and displays it in the **Monitor** pages, such as the **Routing Monitor** or **Quarantine Monitor** pages, in the root FortiGate GUI. You can use the new drop-down menu in the monitor pages to select the device in the Security Fabric that you would like to see monitoring information for.

FortiOS version 5.6

FortiOS version 5.6 includes the following new features and enhancements for the Security Fabric.

Security Fabric dashboard widgets

New dashboard widgets for the Security Fabric allow you to see information about the status of the Security Fabric on the dashboard when you log in to the FortiGate.

Physical and Logical FortiView improvements

The FortiView Physical and Logical Topology pages include many improvements for the Security Fabric, such as showing more devices, displaying link usage in different colors, ranking endpoints, and allowing you to search for specific devices.

FortiClient Vulnerability Score

Endpoints in the Security Fabric topology are now ranked by their FortiClient Vulnerability Score. This score is calculated by the severity of vulnerabilities found on the endpoint.

FortiView consolidation

Information about the Security Fabric can now be seen throughout the FortiView dashboard on the upstream FortiGate when you use the real-time view.

Remote login to downstream FortiGates

You can now log in to downstream FortiGates from the upstream FortiGate, by right-clicking on the downstream FortiGate when viewing the Security Fabric topology using FortiView.

Logging consolidation and improvements

The following changes have been made to improve logging for the Security Fabric:

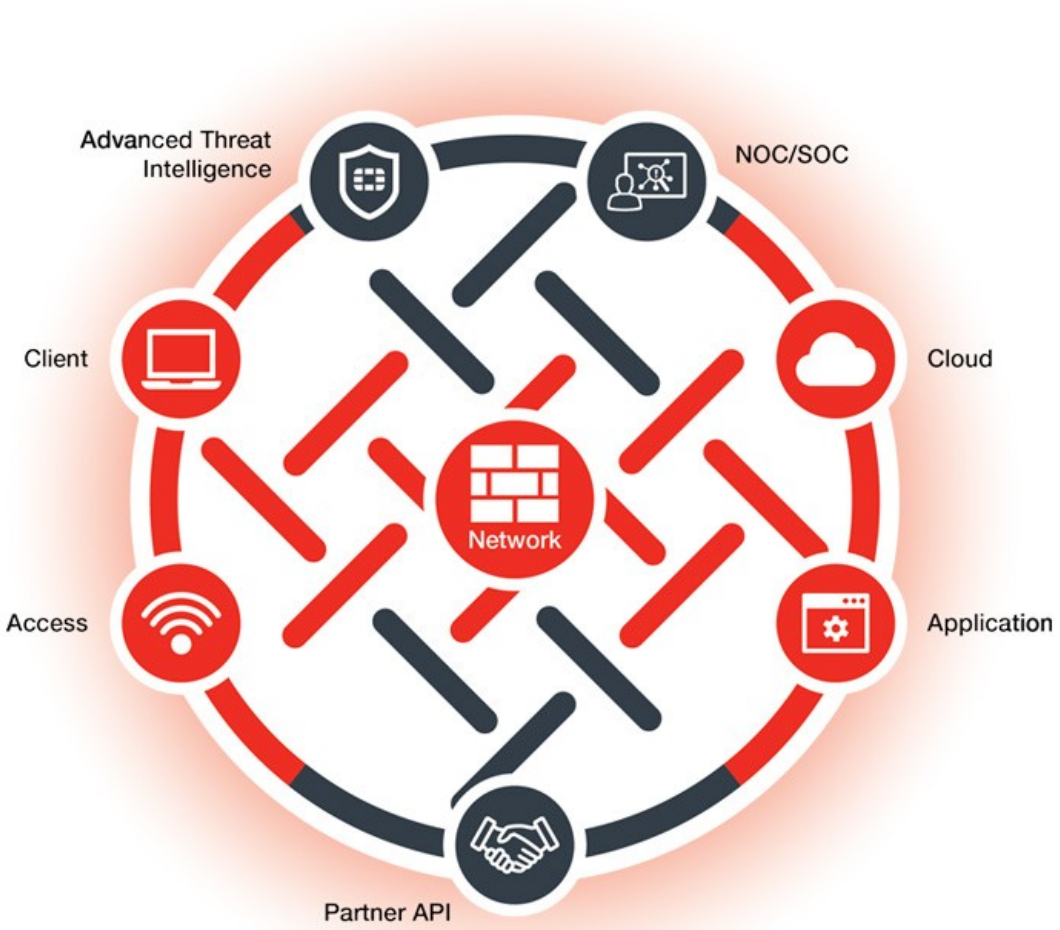
- All FortiGates in the Security Fabric now send logs to a single FortiAnalyzer, by default. You configure the connection to the FortiAnalyzer on the root FortiGate and the settings are then pushed to all other FortiGates in the Security Fabric.
- The following information about the Security Fabric configuration is now sent to the FortiAnalyzer: topology information, interface roles, latitude and longitude information, and device asset tags.
- Monitors on the upstream FortiGate, such as the VPN Monitor, Route Monitor, and User Quarantine, can now view the information from downstream devices.
- You can now see the log statistics for each FortiGate in the Security Fabric.

Device tree

The entire Security Fabric tree is now updated upward and each node has an updated state of the whole subtree.

Security Fabric overview

The Fortinet Security Fabric provides a visionary approach to security that allows your organization to deliver intelligent, powerful, and seamless security. Fortinet offers security solutions for endpoints, access points, network elements, the data center, applications, cloud, and data, designed to work together as an integrated security fabric that can be integrated, analyzed, and managed to provide end-to-end protection for your network. Your organization can also add third-party products that are members of Fortinet's Fabric-Ready Partner Program to the Security Fabric.



All elements in the Security Fabric work together as a team to share policy, threat intelligence, and application flow information. This collaborative approach expands network visibility and provides fast threat detection in real time and the ability to initiate and synchronize a coordinated response, no matter which part of the network is being compromised. The Security Fabric allows your network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

The Security Fabric is designed to cover the entire attack surface and provide you with complete visibility into your network. It allows you to collect, share, and correlate threat intelligence between security and network devices,

centrally manage and orchestrate policies, automatically synchronize resources to enforce policies, and coordinate a response to threats detected anywhere across the extended network. The unified management interface provides you with cooperative security alerts, recommendations, audit reports, and full policy control across the Security Fabric that will give you confidence that your network is secure.

Access security

The Security Fabric secures the access layer of your organization's network. It integrates various access points in a network, such as endpoints, applications, the cloud, and IoT devices, regardless of their distribution, into an end-to-end solution that covers all attack surfaces.

Secure access architecture extends coordinated security policies to the edge of the wired and wireless network, where most vulnerabilities are targeted. It protects the access layer, guarding against data breaches and cybersecurity threats from both internal user devices and IoT products.

Client security

Fortinet's client security, through FortiClient, provides easy-to-manage, automated, fully customizable endpoint security for various devices. FortiClient provides end-to-end threat visibility and control by natively integrating endpoints into the security architecture and offers unified endpoint features, including compliance, protection, and secure access. It also offers integrated patch management and vulnerability shielding to harden all endpoints.

FortiClient integrates with the Security Fabric to provide real-time actionable visibility to stop threats to your organization's network at the endpoints.

For more information about FortiClient, see http://www.forticlient.com/.

Application security

The Security Fabric protects your organization's sensitive and proprietary data that is managed by applications, and ensures the security and availability of your organization's applications. It allows Fortinet application security products, and those of third-party vendors, to work together to boost security across core networks, remote devices, and the cloud. This provides your organization with a network architecture that is secure, aware, actionable, scalable, and open.

Fortinet's robust and integrated application security solution provides a complete end-to-end high-performance solution that protects your organization's valuable information by using a combination of Fortinet products which are deeply integrated into the Security Fabric for direct communications. These products include web application firewalls for application security, DDoS attack mitigation appliances for DDoS protection, advanced application delivery controllers (ADCs) to meet the demands of secure application traffic, sandboxing to isolate malicious code for inspection, and email security gateways that can detect and prevent email-borne threats from getting to your users.

Cloud security

The Security Fabric is designed to extend deep into different cloud environments to ensure that policies are consistent and enforced across all distributed resources. Within the unified security architecture, virtual firewalls can be deployed across private, public, and hybrid clouds to establish north-south and east-west microsegmentation. The Security Fabric weaves cloud applications into the broader environment, governed by seamless, universal security and compliance policies and managed using transparent visibility across the entire attack surface. Combining Fortinet Cloud Security with an existing enterprise firewall deployment extends the same powerful security, as well as the same intelligence and dynamic risk mitigation to applications located either in the cloud or on-premise.

NOC and SOC security

Fortinet's security operations center solution covers both IT and security risk management across your entire organization. The solution is a comprehensive approach to managing risk that includes adaptive awareness of the threat landscape, rapid local and global threat detection, reduced complexity in managing alerts and alarms, and reporting and analytics so you can better understand how your organization's risk profiles are being managed.

When Fortinet devices are unified into a Security Fabric, with compatible operating systems and shared intelligence, the security operations solution also includes information from network elements beyond Fortinet devices. The solution allows your network operations center (NOC) and security operations center (SOC) to share information, integrating and cross-correlating the data from each operations center. This additional context, visibility, and focus breaks down the barrier between your NOC and SOC, and gives you a comprehensive view across your entire Security Fabric so you can quickly find and respond to threats.

Advanced threat intelligence

Fortinet's Advanced Threat Protection (ATP) solution allows your organization to detect and mitigate against threats, both known and unknown, and share that information locally to deliver a coordinated defence.

The ATP solution relies on many types of security technologies, products, and research applied from the network edge through to endpoint devices. To deliver the most effective protection, they are integrated with other security elements from the Enterprise Firewall and Cloud solutions to work together automatically, continuously handing off data from one element to the next to identify, evaluate, and respond to attacks across the entire environment.

The ATP framework delivers end-to-end protection across the attack chain and consists of three elements: prevention, detection, and mitigation, with continuous threat monitoring and analytics from FortiGuard Labs.

For more information about the Advanced Threat Protection Solution, see http://www.fortinet.com/atp.

Partner API

The Fortinet Fabric-Ready Partner Program is an interoperability program for technology alliance partners. Technology alliance partners integrate their products with the Fortinet Security Fabric using Fortinet Security Fabric APIs. Their products are then able to actively collect and share threat and mitigation information from one end of the security solution to the other, which improves threat intelligence, enhances overall threat awareness, and broadens threat response.

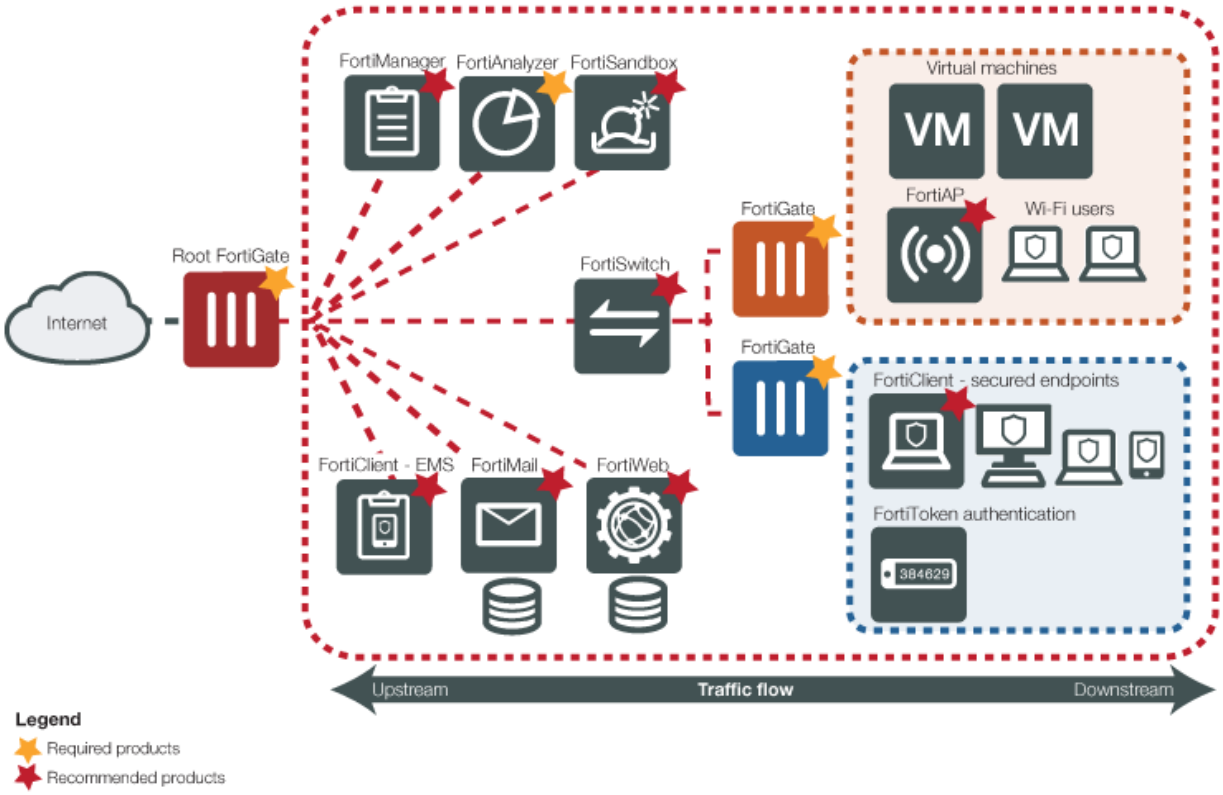
Inclusion in the program means that Fabric-Ready Partners have collaborated with Fortinet and leveraged the Fortinet Security Fabric APIs to develop and validate integrated end-to-end security solutions that are ready for deployment.

The Fabric-Ready Partner Program allows Fortinet technology alliance partners to build on Fortinet products and solutions which help your organization get even more value from your security deployment.

For more information about the Fortinet Fabric-Ready Partner Program, see https://www.fortinet.com/content/dam/fortinet/assets/brochures/Fortinet-Fabric-Partner-Program.pdf.

The Security Fabric solution components

The Fortinet Security Fabric consists of various components that work together to form the Security Fabric that secures your organization's network. The following diagram shows an example Security Fabric that contains both required and recommended Fortinet products:



Devices in the Security Fabric

The Security Fabric implementation consists of required, recommended, and optional devices.

Required devices

The following table shows devices that are required in the Fortinet Security Fabric:

Device	Description
FortiGate	FortiGate is a next-generation firewall (NGFW) that provides enterprise-class protection against network, content, and application-level threats. FortiGates are the core of the Security Fabric and can have one of the following roles in the Security Fabric: • **Root FortiGate**: The root FortiGate is the main component in the Security Fabric. It is typically located on the edge of the network and connects the internal devices and networks to the Internet through your ISP. From the root FortiGate, you can see information about the entire Security Fabric from the Physical and Logical Topology pages in the Security Fabric menu. • **Internal Segmentation Firewall (ISFW)**: After a root FortiGate is installed, all other FortiGates in the Security Fabric act as ISFWs. An ISFW is a firewall that is located at strategic points in your internal network, rather than on the network edge. This allows extra security measures to be taken around key network components, such as servers that contain valuable intellectual property. ISFW FortiGates create network visibility by sending traffic and information about the devices that are connected to them to the root FortiGate.
FortiAnalyzer	FortiAnalyzer collects, analyzes, and correlates log data from Fortinet devices throughout your organization's network, and allows you to view all firewall traffic and generate reports from a single console. FortiAnalyzer gives you increased visibility into your organization's network and simplifies network logging by storing and displaying all log information in one place. It provides centralized monitoring and awareness of threats, events, and network activity by collecting and correlating logs from Security Fabric devices, such as FortiGate, FortiClient, FortiSandbox, FortiWeb, and FortiMail. This gives you a deeper and more comprehensive view across your entire Security Fabric. You can use the robust security alert information and real-time threat intelligence that FortiAnalyzer provides to quickly identify and respond to security threats across your organization's network.

Recommended devices

The following table shows devices that Fortinet recommends you have in the Fortinet Security Fabric:

Device	Description
FortiAP	FortiAP is a wireless access point that provides integrated, secure, identity-driven wireless LAN access for your organization's network. You can add FortiAPs to extend the Security Fabric to your wireless devices. Devices connected to a FortiAP appear in the Physical and Logical Topology pages in the Security Fabric menu.

Device	Description
FortiClient	FortiClient adds endpoint control to devices that are located in the Security Fabric, allowing only traffic from compliant devices to flow through the FortiGate. This is done through FortiClient profiles. In the Security Fabric, FortiClient profiles are applied by the first FortiGate that a device's traffic flows through. This is often an ISFW FortiGate. Device registration and on-net status information for a device that is running FortiClient appears only on the FortiGate that applies the FortiClient profile to the device.
FortiClient EMS	FortiClient Enterprise Management Server (EMS) is a security management solution that provides scalable and centralized management of multiple endpoint devices. FortiClient EMS is used in the Security Fabric to provide visibility across your network, to securely share information and assign security profiles to endpoints.
FortiMail	FortiMail is a secure email gateway that uses various threat prevention methods, including antispam, antimalware, sandboxing, and anomaly detection. FortiMail integrates with other Fortinet products, as well as third-party virtual and cloud platforms, to help establish a seamless Security Fabric across the entire attack surface. FortiMail anti-spam processing helps offload other devices in the Security Fabric that would typically carry out this process.
FortiManager	FortiManager is an easy-to-use, single pane of glass management console, that gives you total visibility, full control, and complete protection of your organization's network. Using the FortiManager in the Security Fabric allows you to simplify the network management of devices in the Security Fabric by centralizing management access in a single device. This allows you to easily control the deployment of security policies, FortiGuard content security updates, firmware revisions, and individual configurations for devices in the Security Fabric.
FortiSandbox	FortiSandbox is an advanced threat protection appliance that improves your security architecture by identifying and validating threats in a separate, secure environment. You can add FortiSandbox to your Security Fabric to improve security with sandbox inspection. Sandbox integration allows FortiGates in the Security Fabric to automatically receive signature updates from FortiSandbox and add the originating URL of any malicious file to a blocked URL list.

Device	Description
FortiSwitch	FortiSwitch is a secure access switch that can be integrated into the Fortinet Security Fabric through the FortiLink protocol. FortiLink allows FortiSwitch ports to become logical extensions of the FortiGate. This allows the FortiGate to auto-discover a connected FortiSwitch for provisioning, including the attachment of policy to ports or VLANs. With an integrated access layer, the FortiGate provides consolidated visibility and reporting with Physical and Logical Topology views of the Security Fabric in the Security Fabric menu. You can add a FortiSwitch to the Security Fabric when it is managed by a FortiGate within the Security Fabric, and connected to an interface that uses FortiTelemetry. Devices connected to the FortiSwitch appear in the Physical and Logical Topology pages in the Security Fabric menu, and security features, such as FortiClient profiles, are applied to them.
FortiWeb	FortiWeb is a web application firewall that protects hosted web applications from attacks that target known and unknown exploits. In the Security Fabric, FortiWeb defends the application attack surface from attacks that target application exploits. You can also configure FortiWeb to apply web application firewall features, virus scanning, and web filtering to HTTP traffic to help offload other devices in the Security Fabric that would typically carry out these processes.

Optional devices

The following table shows devices that are optional in the Fortinet Security Fabric:

Device	Description
Other Fortinet products	Many other Fortinet products can be added to the Security Fabric, including FortiAuthenticator, FortiToken, FortiCache, and FortiSIEM.
Third-party products	Third-party products that belong to the Fortinet Fabric-Ready Partner Program.

Security Fabric topology views

You can see the Security Fabric topology in the root FortiGate GUI. Two viewing options are available: the Physical Topology view and the Logical Topology view.

The Physical Topology view displays the physical structure of your network, by showing the devices in the Security Fabric and the connections between them. The Logical Topology view displays the logical structure of your network, by connection, by showing information about logical and physical network interfaces in the Security Fabric and the interfaces that connect devices in the Security Fabric. Only Fortinet devices are shown in the topology views.

For more information about the topology views, see Viewing the Security Fabric topology.

Security Fabric Audit

The Security Fabric Audit provides a method to continually monitor and improve your organization's Security Fabric configuration. The Security Fabric Audit is a feature on the FortiGate that analyzes your Security Fabric deployment, identifies potential vulnerabilities, and highlights best practices that you can use to improve the overall security and performance of your network. Using the Security Fabric Audit helps you to:

- Tune your network configuration
- Deploy new hardware and software
- Have more visibility into your network
- Gain more control over your network
- Adhere to your organization's compliance requirements

The Security Fabric Audit provides a Security Fabric Score based on how many checks your network passes and fails during the Security Fabric Audit. By checking the Security Fabric Score, and implementing the recommendations, you can have confidence that your network is getting more secure over time.

For more information about running a Security Fabric Audit, see Running a Security Fabric Audit.

FortiTelemetry

FortiTelemetry is a protocol that Fortinet products in the Security Fabric use to communicate with each other. It connects Security Fabric devices and allows dynamic status updates to travel between them. The Security Fabric uses FortiTelemetry to link various security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs in your network in real time.

You must enable FortiTelemetry on interfaces that connect Fortinet devices in the Security Fabric.

Configuring the Security Fabric

To configure the Security Fabric, you must form the Security Fabric and then set up data collection for the Security Fabric.

Setting up data collection includes configuring the FortiAnalyzer so that the entire Security Fabric is recognized by the FortiAnalyzer. Once this is done, the root FortiGate and downstream FortiGates can show information about all downstream FortiGates and other devices that are connected to them. Then you can use the Security Fabric features to view, assess, and improve your organization's network security.

System requirements

To set up the Security Fabric in FortiOS 5.6, the devices that you want to include in the Security Fabric must meet the following requirements. Some features of the Security Fabric are available only in certain firmware versions.

Device	Requirement	Feature conditions
FortiGate	• Version 5.6 and later • All ISFW FortiGates should be running the same firmware version as the root FortiGate • FortiGate is a required device in the Security Fabric	
FortiAnalyzer	• Version 5.6 and later • Logging to the FortiAnalyzer must be enabled • FortiAnalyzer is a required device in the Security Fabric	
FortiClient	Version 5.6 and later	
FortiClient EMS	Version 1.2 and later	
FortiAP	Version 5.4 and later	Version 5.6 and later is recommended to access all features
FortiSwitch	Version 3.5.2 and later	Version 3.5.3 and later is recommended to access all features

For more information about upgrading the Security Fabric to version 5.6, see the Security Fabric Upgrade guide.

Prerequisites

- Determine which devices you want to have in the Security Fabric
- Ensure devices meet the System requirements
- If devices are not already installed in your network, complete basic installation and configuration tasks by following the instructions in the device documentation
- Disable virtual domains (VDOMs) on all FortiGates that you want to add to the Security Fabric

Forming the Security Fabric

To form the Security Fabric, you configure the root FortiGate and then the ISFW FortiGates. Although you can configure any of the FortiGates in the Security Fabric to be the root FortiGate, you typically configure the edge FortiGate as the root FortiGate. This setup allows you to view the full topology of the Security Fabric from the top down.

The following procedures include configuration steps for a typical Security Fabric implementation, where the root FortiGate is the edge FortiGate and the ISFW FortiGates are all FortiGates that are downstream from the root FortiGate.

Configure the root FortiGate for the Security Fabric

1. In the root FortiGate GUI, select **Security Fabric** > **Settings**.
2. In the Security Fabric Settings page, enable **FortiGate Telemetry**.
3. In the **Group name** field, set a name for the Security Fabric group.
4. In the **Group password** field, set a password for the Security Fabric group.
5. Ensure that **Connect to upstream FortiGate** is disabled.
6. In the **FortiTelemetry enabled interfaces** field, add the interfaces on this FortiGate that listen for downstream Security Fabric connections.
   The **FortiAnalyzer Logging** setting is automatically enabled.
7. In the **IP address** field, enter the IP address of the FortiAnalyzer that you want the Security Fabric to send logs to. If you select **Test Connectivity**, and this is the first time that you are connecting the FortiGate to the FortiAnalyzer, you will receive an error message because the FortiGate has not yet been authorized on the FortiAnalyzer. You can configure this authorization when you configure the FortiAnalyzer.
8. In the **Upload option** field, select the option for how often you want the FortiGate to send logs to the FortiAnalyzer.
9. If you want log transmissions encrypted, enable the **Encrypt log transmission** option. The log transmissions are encrypted using SSL.
10. Select **Apply**.

Configure ISFW FortiGates for the Security Fabric

1. In the ISFW FortiGate GUI, select **Security Fabric** > **Settings**.
2. In the Security Fabric Settings page, enable **FortiGate Telemetry**.
3. In the **Group name** field, enter the group name that you set for the Security Fabric.
4. In the **Group password** field, enter the group password that you set for the Security Fabric.
5. Enable the **Connect to upstream FortiGate** option.
6. In the **FortiGate IP** field, enter the IP address of the port on the upstream FortiGate that this FortiGate connects to. Depending on your network topology, the upstream FortiGate is another ISFW FortiGate or the root FortiGate. The FortiAnalyzer setting is automatically enabled. Settings for the FortiAnalyzer will be retrieved when the ISFW FortiGate connects to the root FortiGate.
7. Select **Apply**.
8. Repeat this procedure on every ISFW in the Security Fabric.

Setting up data collection for the Security Fabric

To set up data collection for the Security Fabric, you enable device detection on ISFW FortiGates and then connect the FortiAnalyzer to the Security Fabric.

You enable device detection on the interfaces of the ISFW FortiGates where you want the devices attached to those interfaces added to the Security Fabric. Only devices detected on those interfaces are shown in the Security Fabric topology views.

Connecting the FortiAnalyzer to the Security Fabric allows the Security Fabric to show historical data for the Security Fabric topology and logs for the entire Security Fabric.

Enable device detection on ISFW FortiGates

1. In the ISFW FortiGate GUI, select **Network** > **Interfaces**.
2. Select the interface that you want to enable device detection on.
3. Select **Edit**.
4. In the **Addressing mode** field, select **Manual**.
5. In the **IP/Network Mask** field, enter a private IP address and network mask.
6. If you have FortiClient clients behind this interface, in the **Administrative Access** section, enable **FortiTelemetry**.
7. If you require the FortiGate to provide IP addresses using DHCP to devices that connect to this interface, enable **DHCP Server**. Suitable address ranges are automatically created.
8. In the **Networked Devices** section, enable **Device Detection**.
9. Select **OK**.
10. Repeat this procedure for every interface that you want to enable device detection on.

Connect the FortiAnalyzer to the Security Fabric

Ensure that all FortiGates in the Security Fabric are registered with the same FortiAnalyzer.

1. In the FortiAnalyzer GUI, select **System Settings** > **Network**.
2. Select **All Interfaces**.
3. Select the port that connects to the root FortiGate.
4. Select **Edit**.
5. In the **IP Address/Netmask** field, enter the IP address used for the Security Fabric configuration on the root FortiGate.
6. In the **Default Gateway** field, enter the IP address of the interface on the root FortiGate that the FortiAnalyzer connects to.
7. Select **OK**.
8. Select **System Settings** > **Device Manager**.
   The FortiGates are listed as **Unregistered**.
9. Select the root FortiGate and the ISFW FortiGates in the Security Fabric.
10. Select **+ Add Device**.
    The FortiGates are now listed as **Registered**.
    A warning icon will appear beside the root FortiGate, because the FortiAnalyzer requires administrative access to the root FortiGate in the Security Fabric.
11. In the **Authentication** window, complete the **Admin User** and **Password** fields to authenticate the Security Fabric.
    After the FortiAnalyzer authenticates the Security Fabric, the FortiAnalyzer shows the full Security Fabric topology.

You can verify that the FortiAnalyzer configuration is successful by selecting **Security Fabric** > **Settings** on the root and ISFW FortiGates. The **Storage usage** field in the **FortiAnalyzer Logging** section should now show storage usage information.

Using the Security Fabric to improve network security

Once you set up the Security Fabric, there are various Security Fabric features that you can use to improve your network security, including the following:

- Dashboard widgets
- Topology views
- Security Fabric Audit
- Monitoring views

Understanding the Security Fabric dashboard widgets

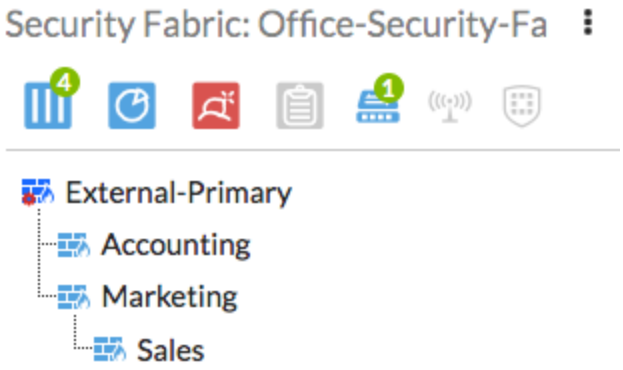
You can add Security Fabric widgets to the dashboard on the root FortiGate. There are two widgets available: the Security Fabric widget and the Security Fabric Score widget. The widgets allow you to see information about the status of the Security Fabric when you first log in to the FortiGate.

If either of these widgets do not appear on your dashboard, you can add them using the settings button in the bottom right corner. This button appears when your mouse hovers over any part of the dashboard.

On the root FortiGate, select **Dashboard** > **Main**.

The Security Fabric widget

The Security Fabric widget shows a visual summary of many of the devices in the Security Fabric. You can hover over the icons at the top of the widget to get a quick view of the status of the Security Fabric, including the status of FortiTelemetry and devices in the Security Fabric.



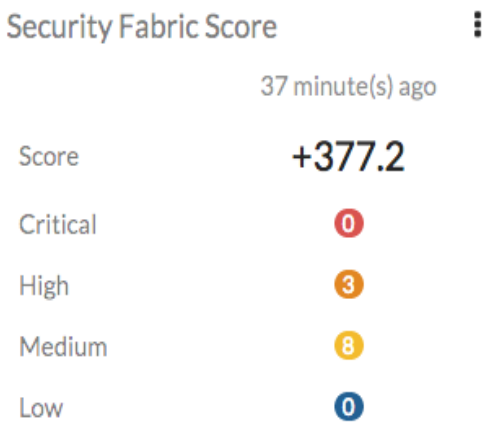
The widget shows the following information:

- The name of your Security Fabric
- Icons indicating the other Fortinet devices that can be used in the Security Fabric:
  - Devices in blue are detected in your network
  - Devices in gray are not detected in your network
  - Devices in red are not detected in your network, but are recommended for the Security Fabric

- The names of the FortiGates in the Security Fabric

The Security Fabric Score widget

The Security Fabric Score widget shows the latest Security Fabric Audit score and allows you to apply audit recommendations from the dashboard.



The widget shows the following information:

- The time that the score was last calculated
- The Security Fabric score
- A list of the number of checks that were not passed, ranked by the following severities: Critical, High, Medium, and Low

Viewing the Security Fabric topology

You can see the Security Fabric topology in the FortiGate GUI, in the Security Fabric menu. You can choose the Physical Topology or Logical Topology views. In both topology views, you can hover over device icons and use filtering and sorting options to see more information about devices and your organization's network. To view the complete network, you must access the topology views on the root FortiGate in the Security Fabric.

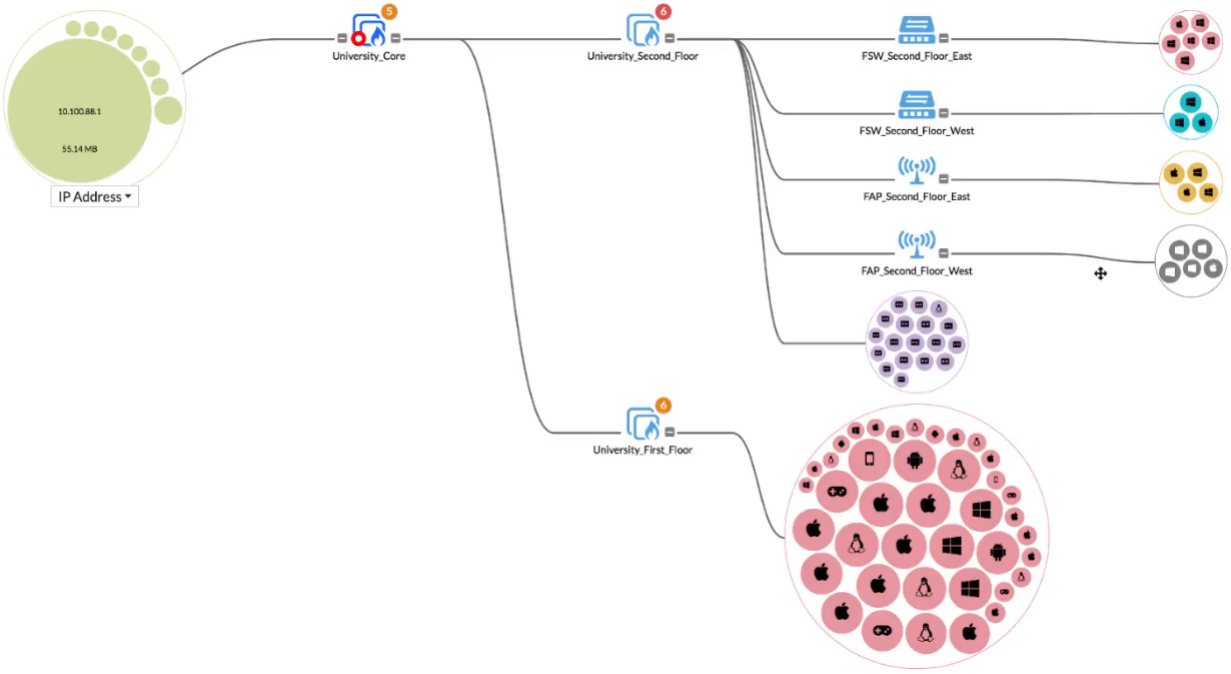
You can also see the Security Fabric topology in the FortiAnalyzer GUI. In the FortiAnalyzer GUI, select **Device Manager**. The FortiGates in the Security Fabric are shown as part of a Security Fabric group. An asterisk (*) appears beside the root FortiGate in the Security Fabric. To see the topology of the Security Fabric, right-click on the Security Fabric group and select **Fabric Topology**.

Only Fortinet devices are shown in the Security Fabric topology views.

View the Physical Topology

The Physical Topology view shows the devices in the Security Fabric and the devices they are connected to. You can also select whether or not to view access layer devices in this topology.

To see the Physical Topology, in the root FortiGate GUI, select **Security Fabric** > **Physical Topology**.



The Physical Topology view displays your network as a bubble chart of interconnected devices. These devices are grouped based on the upstream device they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to resize it and view more information about the device.

FortiGates and other networking devices are depicted as boxes. You can hover over the icon for each FortiGate to see information, such as serial number, hostname, and firmware version. You can hover over the bubbles of other devices to see information about them, such as name, IP address, and traffic volume data.

Security Fabric Audit recommendations are also shown in the topology, beside the icon of the device the recommendations apply to.

View the Logical Topology

The Logical Topology view is similar to the Physical Topology view, but it shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric.

To see the Logical Topology, in the root FortiGate GUI, select **Security Fabric** > **Logical Topology**.

The Logical Topology view displays your network as a bubble chart of network connection points. These devices are grouped based on the upstream device interface they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to re-size it.

FortiGates and other networking devices are depicted as boxes. You can hover over the icon for each FortiGate to see information, such as serial number, hostname, and firmware version. You can also see each FortiGate

interface that has upstream and downstream devices connected to it. You can hover over the name of an interface to see its IP address, network (subnet), and role.

Security Fabric Audit recommendations are also shown in the topology, beside the icon of the device the recommendations apply to.

Filter the topology views by specific criteria

You can use filters to narrow down the data on the topology views, so you can find specific information.

1. In the drop-down menu to the right of the **Search** field, select one of the following:
   - Device Traffic
   - Device Count
   - Device Type
   - Vulnerability
   - Threat Score
   - No Device
2. To filter the view by time, in the time period drop-down menu, select one of the following:
   - now
   - 5 minutes
   - 1 hour
   - 24 hours
   - 7 days
3. To sort the topology by traffic options, in the **Sort By** drop-down menu, select one of the following:
   - Bytes (Sent/Received)
   - Packets (Sent/Received)
   - Bandwidth
   - Session

Running a Security Fabric Audit

You can run a Security Fabric Audit to analyze your organization's Security Fabric deployment, identify potential vulnerabilities, and highlight best practices that you can use to improve the overall security and performance of your organization's network.

The Security Fabric Audit performs a variety of checks when it analyzes your network. All checks are based on your current network configuration, using real-time monitoring. The audit runs the checks across all FortiGates in the Security Fabric.

When the audit is complete, a list of recommendations is shown. Two views are available: Failed or All Results. You can filter these views further in order to view results from a specific FortiGate or all FortiGates. Each view has a chart that shows the results of individual checks, and includes the name and a description of the check, which FortiGate the check was performed on, the impact of the check on the overall security score, and recommendations. If you hover over the result for a check, you can see a breakdown of how the score was determined.

You can choose to automatically apply the recommendations that include the Easy Apply option. By using Easy Apply, you can change the configuration of any FortiGate in the Security Fabric. Further action is required if you want to follow other recommendations.

You can also view audit recommendations for specific devices in the Physical and Logical Topology views in the Security Fabric menu. If a recommendation is available for a device, a circle containing a number appears. The number shows how many recommendations are available. The color of the circle shows the severity of the highest check that failed. The following table shows the severity that each color represents:

Color	Severity
Red	Critical
Orange	High
Yellow	Medium
Blue	Low

For more information about the Security Fabric Audit, and details about each of the audit checks that are performed, see the Fortinet Recommended Security Best Practices document.

Run a Security Fabric Audit

You must run the Security Fabric Audit on the root FortiGate in the Security Fabric.

1. In the root FortiGate GUI, select **Security Fabric** > **Audit**.
   In the **Detect Security Fabric FortiGates** step, all FortiGates in the Security Fabric are listed.
2. To run the audit, select **Next**.
   The Audit will run. When it completes, the **Audit** step is displayed, which shows the following information:
   - The **Security Score** field shows the score for your Security Fabric
   - The page shows the overall count of how many checks passed or failed, with the failed checks divided by severity
   - Information about each failed check, including which FortiGate failed the check, the effect of the check failure on the security score, and recommendations to fix the issue
   - The **Easy Apply** option appears with recommendations that can be automatically applied by the wizard
3. To move to the **Easy Apply** option page, select **Next**.
4. Select all recommendations that you want to implement in the Security Fabric.
5. Select **Apply Recommendations**.

Set up logging for the Security Fabric Audit

You can configure an event filter subtype for the Security Fabric Audit. When you run an audit, event logs are created on the root FortiGate that summarize the results of the audit and show detailed information for the individual tests.

To configure logging for the Security Fabric Audit, use the following CLI commands:

```
config log eventfilter
   set security-audit {enable | disable}
end
```

Understanding the Security Fabric Score

When you run a Security Fabric Audit, your organization's Security Fabric receives a Security Fabric Score. The score will be positive or negative, and a higher score represents a more secure network.

The score is based on how many checks your network passes and fails, as well as the severity level of these checks. The following table shows the weight for each severity level:

Severity level	Weight
Critical	50 points
High	25 points
Medium	10 points
Low	5 points

The audit awards points when a check passes, using the following formula:

+ <Severity Weight> x *<Secure FortiGate Multiplier>*

where:

- *Severity Weight* is *<Severity level>* / *<number of FortiGates in the Security Fabric>*
- *Secure FortiGate Multiplier* is determined using logarithms and the number of FortiGates in the Security Fabric

For example, if you have four FortiGates in the Security Fabric, and all of them pass the Compatible Firmware check, the score for each FortiGate is calculated as: (50/4) x 1.292 = 16.2 points.

All FortiGates in the Security Fabric must pass the check in order to receive points. If any of the FortiGates in the Security Fabric fail a check, any FortiGates in the Security Fabric that passed the check are not awarded points. For the FortiGate that failed the test, the score is calculated using the following formula:

- <Severity Weight> x *<Count>*

where:

- *Severity Weight* is *<Severity level>*
- *Count* is the number of times the check failed during the audit

For example, if the audit finds two critical FortiClient vulnerabilities, the score for that check is calculated as: -50 x 2 = -100 points.

The score is not affected by checks that do not apply to your network. For example, if you do not have any FortiAPs in the Security Fabric, you will not receive any points for the FortiAP Firmware Versions check.

Viewing monitoring information for devices in the Security Fabric

The Security Fabric retrieves monitoring information from all devices in the Security Fabric and displays it in the monitor pages in the root FortiGate GUI.

View monitoring information for a specific device in the Security Fabric

1. In the root FortiGate GUI, select **Monitor**.
2. Select the monitor page that you want to view. For example, **Routing Monitor** or **Quarantine Monitor**.
3. In the drop-down menu, select the device in the Security Fabric that you want to see monitoring information for.

Related resources

Document	Location
Security Fabric documentation	http://docs.fortinet.com/security-fabric/admin-guides
The Security Fabric Cookbook Recipe Collection	http://cookbook.fortinet.com/security-fabric-56/
Security Fabric Upgrade Guide	http://docs.fortinet.com/fortigate/release-information
Fortinet Communication Ports and Protocols Guide	http://docs.fortinet.com/d/fortinet-communication-ports-and-protocols-56
FortiGate documentation	http://docs.fortinet.com/fortigate/admin-guides
FortiAnalyzer documentation	http://docs.fortinet.com/fortianalyzer/admin-guides
FortiAP documentation	http://docs.fortinet.com/fortiap/admin-guides
FortiClient documentation	http://docs.fortinet.com/forticlient/admin-guides
FortiClient EMS documentation	http://docs.fortinet.com/ems/admin-guides
FortiMail documentation	http://docs.fortinet.com/fortimail/admin-guides
FortiManager documentation	http://docs.fortinet.com/fortimanager/admin-guides
FortiSandbox documentation	http://docs.fortinet.com/fortisandbox/admin-guides
FortiSwitch documentation	http://docs.fortinet.com/fortiswitch/admin-guides
FortiWeb documentation	http://docs.fortinet.com/fortiweb/admin-guides